MALFEASANT USE PREVENTING SYSTEM FOR PORTABLE TERMINAL EQUIPMENT

Patent Number: JP3100895

Publication date: 1991-04-25

Inventor(s): TAKAHASHI TAKEHIRO; others: 07

Applicant(s): HITACHI MAXELL LTD; others: 01

Requested Patent: ☐ JP3100895

Application Number: JP19890239016 19890914

Priority Number(s):

IPC Classification: G08B15/00; G06F15/00; G06F15/30; G06F15/74; G06K17/00; G08B13/00; G08B21/00; G08B23/00

EC Classification:

Equivalents:

Abstract

PURPOSE:To prevent malfeasant use from being performed when burglary occurs by starting the monitor of a time monitoring means setting the extraction time of an IC card as reference, and operating a normal operation stopping means by the detection of the time monitoring means when no IC card is loaded for prescribed time.

CONSTITUTION:The above system is equipped with the time monitoring means 8 and the normal operation stopping means 1, 3b, and the start of the monitoring time of the time monitoring means 8 is set at the extraction time of the IC card 20. When no IC card 20 is loaded for the prescribed time, the normal operation stopping means 1, 3b are operated by the detection of the time monitoring means 8, and for example, the normal data processing of portable terminal equipment can be blocked by erasing an input processing program and nullifying stored data. Thereby, the malfeasant use can be prevented from being performed when the burglary occurs.

circuit 8, the anti-theft program 3a causes a processing program such as an input data processing program 3c or the like to overrun to thereby active the operation suspension program 3b.

With the theft flag 14 raised, the operation suspension program 3b invalidates or erase data in a predetermined region in the memory 3 to suspend operation of the settlement terminal 10 and, moreover, erases the input data processing program 3c stored in the memory 3. This makes it impossible to apply processing, such as input or output, with respect to data stored, as a result of which the device does not operate normally. When the theft flag 14 is not raised, meaningless data may be written in an input data storing region in a mounted IC card 20 or memory 3 or the processing program may be caused to overrun, to thereby prevent the device from performing normal operation.

Here, the time monitoring circuit 8 is controlled by the microprocessor 1. When the microprocessor 1 confirms that the mounted IC card 20 has a particular code, the microprocessor 1 causes the time monitoring circuit 8 to suspend time monitoring and resets the measured time value to zero. When the microprocessor 1 detects a situation in which no IC card having the particular code is mounted or such an IC card has been removed, the microprocessor 1 sends an activation signal to the time monitoring circuit 8 to have it start time measuring. Note that a time for the time monitoring circuit 8 to monitor can be desirably set by the microprocessor 1, and the setting is achieved using an input from an input device 5. Whether or not the IC card has a particular code is determined by reading out an ID code attached to the IC card to verify relative to an ID code 15.

The above-constructed settlement terminal 10 may be installed, for example, as an IC card shopping terminal device in a register in a supermarket for use as a terminal which writes product

purchase money data in an IC card of a predetermined customer to attain cashless shopping. In this case, identical data to the data written in the IC card is stored in the terminal device as back-up data, and a corresponding amount of money is debited later from the customer's bank account. Therefore, in this system, a person in charge of registers, or the like, itinerates the registers for every two hours, for example, while carrying a dedicated IC card, and loads the IC card to the terminal device to record the various data, including the above-mentioned data, stored in the terminal device in the IC card.

Suppose that the setting time of the time monitoring circuit 8 is 2.5 hours in this system. In this case, when an IC card with a particular code is not loaded by the person in charge after 2.5 hours have elapsed, the time monitoring circuit 8 sends an interruption signal to the microprocessor 1 to activate the anti-theft program 3a, and further the operation suspension program 3b. As a result, a processing program in the settlement terminal 10 overruns or meaningless data is written in an IC card mounted or stored in the memory 3. Then, only when the particular IC card indicative of the person in charge is loaded, the time monitoring is suspended with the monitored time returned to zero. Note that, because time monitoring is suspended only when an IC card indicative of a person in charge is loaded in this case, time monitoring should be set suspended during a night time according to a predetermined procedure, and the terminal device may be saved in a safety box or the like.

Here, in a case where the settlement terminal 10 is stolen and taken out of the supermarket, there is a risk that the purchase money data which is stored as back-up in the terminal device may be analyzed and that balance data in the IC card may be manipulated. In order to prevent this risk, the system is designed such that the signal transmitting device 21 emits predetermined electric waves in the supermarket so that the

settlement terminal 10 continuously receives signals via its plate-like antenna 8 in the terminal device. When the settlement terminal 10 is stolen and taken out of the supermarket, the radio wave strength detection circuit 7 of the settlement terminal 10 detects a drop in strength of the received electric wave to below a predetermined level. An interruption signal resulting from the detection signal causes the microprocessor 1 to activate the anti-theft program 3a and further the operation suspension program 3b to thereby set a theft flag 14 and give an alarm, so that the stored back-up data and the input data processing program 3d are erased. With the above, the stored data will not be read out and used illegally. In addition, since a part of the processing program of the terminal device is erased, the terminal device does not operate normally.

Such a settlement terminal 10 may be used as an IC card working hour management terminal device. An example of such a use will be described. Note that in this case, an interruption by a detection signal from the time monitoring circuit 8 is treated equally to an interruption by the radio wave strength detection circuit 7. Instead of the time monitoring circuit 8 releasing time measuring in response to detection of presence/absence of a particular IC card, input of a particular secret ID code from the input device 5 causes to release time measuring.

The IC card working hour management terminal device records data regarding the time at which an individual arrives at or leaves a workplace, or the like, in an IC card loaded thereto by the individual arriving at or leaving the working place. The IC cards are collected once a month so that the recorded arrival and leaving times are read out for calculation of the working hours. Similar to the above, identical data to that which is recorded in the IC card is recorded as back-up in the IC card working hour management terminal device. When the terminal device is stolen, there is a risk that the data recorded in the

IC card can be manipulated. In order to prevent this risk, a person in charge inputs a secret IC code in the terminal device every three hours via the input device 5. The working hour management terminal device compares the input secret IC code and a code stored inside (corresponding to an ID code 15) to determine if the input code is a code for releasing a monitored time by the time monitoring circuit 8. When the codes match to each other, the working hour management terminal device controls the time monitoring circuit 8 to reset the measured time. Note that suppose that a setting time for the time monitoring circuit 8 is four hours here.

The terminal device monitors four hours, and, when no secret ID code is input even after four hours has passed, determines that the terminal device has been stolen. Then, the terminal device activates the anti-theft program 3a by means of interruption by the time monitoring circuit 8. Then, the operation suspension program 3b is also activated to give an alarm. As a result, it is known that a person who has stolen the device possesses the terminal device. Only when a correct secret IC number is input, time monitoring by the terminal device can be returned to the initial state. Note that, similar to the above, time monitoring may be set suspended or set with a long time during a night time. This setting is achieved using a particular code. Then, the terminal device can be saved in a safety box.

It should be noted that, although only an IC card having a specific code can make time monitoring to be returned to the initial state, as described above, in this embodiment, it is not necessary to be achieved using a particular IC card.

Moreover, beside what is described in the above, such processing may be applied as a normal operation suspension means, that invalidates information on a key which is input from the terminal device.

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平3−100895

⑤Int.Cl.[5]	識別記号	庁内整理番号
G 08 B 15/00		7605−5C
G 06 F 15/00	330 A	7218−5B
15/30	330	6798−5B※

⑬公開　平成3年(1991)4月25日

審査請求　未請求　請求項の数 3　(全6頁)

⑭発明の名称　携帯用端末装置の不正使用防止方式

⑳特　願　平1−239016

㉒出　願　平1(1989)9月14日

㉑発明者　高橋　武博　大阪府茨木市丑寅1丁目1番88号　日立マクセル株式会社内

㉑発明者　橘田　謙一　大阪府茨木市丑寅1丁目1番88号　日立マクセル株式会社内

㉑発明者　品川　徹　大阪府茨木市丑寅1丁目1番88号　日立マクセル株式会社内

㉑出願人　日立マクセル株式会社　大阪府茨木市丑寅1丁目1番88号

㉑出願人　株式会社日立製作所　東京都千代田区神田駿河台4丁目6番地

㉔代理人　弁理士　梶山　佶是　外1名

最終頁に続く

明　細　書

1.発明の名称

携帯用端末装置の不正使用防止方式

2.特許請求の範囲

(1) データの入力手段と表示手段とを有し、ICカードが装着されて、このICカードとデータの授受を行う携帯用端末装置において、設定された監視時間までにICカードが装着されないときにこれを検出して検出出力を発生する時間監視手段と、前記検出出力に応じて正常な動作を停止させる正常動作停止手段とを備え、前記時間監視手段はICカードが装着されているときにその動作を停止し、ICカードが抜去されたときから前記監視時間についての時間計測を開始することを特徴とする携帯用端末装置の不正使用防止方式。

(2) 外部装置から送信された電波をアンテナを介して受信してその電波の強度を検出する検出回路を有していて、その強度が一定レベル以下になったときには正常動作停止手段が起動されることを特徴とする請求項1の記載の携帯用端末装置の不正使用防止方式。

(3) データの入力手段と表示手段とを有し、ICカードが装着されて、このICカードとデータの授受を行う携帯用端末装置において、設定された監視時間までに特定のコードが前記入力手段から入力されないときにこれを検出して検出出力を発生する時間監視手段と、前記検出出力に応じて正常な動作を停止させる正常動作停止手段とを備え、前記時間監視手段は前記特定のコードが入力されたときに前記監視時間の時間計測を初期状態に戻し、初期状態から時間計測をすることを特徴とする携帯用端末装置の不正使用防止方式。

3.発明の詳細な説明

[産業上の利用分野]

この発明は、携帯用端末装置の不正使用防止方式に関し、詳しくは、ICカードを利用してデータの授受を行う携帯用端末装置において、盗難にあったときにその盗難にあった装置のデータを無効にして正常に動作しないようにすることができるような不正使用防止方式に関する。

〔従来の技術〕

従来、銀行や各種の金融機関で使用されている現金取引装置等の端末装置は大型なものが用いられ、通常、オンラインで動作することから盗難の危険性はほとんどないが、最近では、このような端末装置もＬＳＩの高機能化や高集積化に伴って小型化されてきている。これとは別に機動性や個別性が重視され、家庭や出先で使用され、現金取引とか、振込等の銀行端末業務等の処理が行われる携帯用の端末装置が普及してきている。また、ＩＣカード等を使ったオフラインの携帯用端末装置も使用されつつある。

〔解決しようとする課題〕

このように、端末装置が小型化し、携帯性に優れ、かつ、高機能なものが普及してくると、正当な使用者でない他人が端末装置を持ち去り、それが悪用される危険性も増加する。しかも、その悪用が現金等の出し入れや振替等に関する不正であるときには被害も大きくなり、社会に与える影響も大きい。

この発明は、このような従来技術の問題点を解決するものであって、携帯用端末装置が盗難にあったときに悪用されないようにすることができる携帯用端末装置の不正使用防止方式を提供することを目的とする。

〔課題を解決するための手段〕

このような目的を達成するためのこの発明の携帯用端末装置の不正使用防止方式の構成は、データの入力手段と表示手段とを有し、ＩＣカードが装着されて、このＩＣカードとデータの授受を行う携帯用端末装置において、設定された監視時間までにＩＣカードが装着されないときにこれを検出して検出出力を発生する時間監視手段と、検出出力に応じて正常な動作を停止させる正常動作停止手段とを備えていて、時間監視手段がＩＣカードが装着されているときにその動作を停止し、ＩＣカード抜去されたときから監視時間についての時間計測を開始するものである。

また、同様な目的を達成する他の発明の構成は、データの入力手段と表示手段とを有し、ＩＣカードが装着されて、このＩＣカードとデータの授受を行う携帯用端末装置において、設定された監視時間までに特定のコードが前記入力手段から入力されないときにこれを検出して検出出力を発生する時間監視手段と、検出出力に応じて正常な動作を停止させる正常動作停止手段とを備えていて、時間監視手段が特定のコードが入力されたときに監視時間の時間計測を初期状態に戻し、初期状態から時間計測をするものである。

〔作用〕

このように、時間監視手段の監視時間の開始をＩＣカードの抜去時点を基準とすることにより、ＩＣカードが所定時間の間装着されないときには時間監視手段の検出により正常動作停止手段が動作して、これによって、例えば、入力処理プログラムを消去し、記憶したデータを無効とすることで携帯用端末装置の正常なデータ処理が阻止されるので、盗難にあっても不正利用されなくても済む。

なお、前記のＩＣカードに換えて、入力装置から特定のコードを入力するようにして時間監視手段の時間計測を解除して初期状態に戻すようにしても同様の効果が得られる。

〔実施例〕

以下、この発明の一実施例について図面を参照して詳細に説明する。

第１図は、この発明の携帯用端末装置の不正使用防止方式を適用したＩＣカード精算処理端末装置のブロック図であり、第２図は、その外観図である。

第１図，第２図において、１０は、携帯用ＩＣカード精算処理端末装置（以下精算処理端末）であって、ＩＣカード２０との間でデータの授受を行う。

精算処理端末１０は、内部にマイクロプロセッサ１と、クロック発振回路２、メモリ３、表示装置４、入力装置５、外部の電波による信号送信装置２１から送信された電波を受信するアンテナ８、このアンテナ８を介して受信してそのレベルが一定値以下になったときにこれを検出する電波強度

検出回路7、時間監視回路8、ICカードインタフェース9、マイクロプロセッサ1により駆動される警報回路（ブザー）12等とを備えていて、ICカードインタフェース9はICカードコネクタ9aに接続されている。なお、13は、精算処理端末10に挿填された電池である。

マイクロプロセッサ1と、メモリ3、表示装置4、入力装置5、ICカードインタフェース9、警報回路12とは、相互にバス11を介して接続されていて、電波強度検出回路7と時間監視回路8とは、それぞれマイクロプロセッサ1のそれぞれに対応する割込み端子に接続され、マイクロプロセッサ1に割込み信号を送出する。また、メモリ3には、後述するような各種プログラムとこの時間監視回路8が計測した時間をゼロに戻す処理をするときに、装着されたICカードの正当性を認識するための識別コード15とが格納されている。

先の各種プログラムとしては、電波強度検出回路7及び時間監視回路8のそれぞれからマイクロプロセッサ1に加えられた割込み信号で起動される対盗難処理プログラム3aと、メモリ3の所定領域に記憶された盗難フラグ14が立てられたときにメモリ3に記憶された所定のプログラムを消去し、また、所定のデータを無効にする動作停止処理プログラム3bと、メモリ3上の消去可能な領域、例えば、データ記憶領域に記憶された入力データ処理プログラム3c等が格納されている。なお、対盗難処理プログラム3aと動作停止処理プログラム3bとは、メモリ3ではなく、マイクロプロセッサ1のROMに格納されていてもよい。

ここで、対盗難処理プログラム3aは、電波強度検出回路7からの検出信号により割込みを受けたときは、盗難フラグ14をメモリ3の所定領域に立てて（例えば、フラグを"0"から"1"にセットして）警報回路15と動作停止処理プログラム3bとを起動する。また、時間監視回路8からの検出信号により割込みを受けたときには、入力データ処理プログラム3c等の処理プログラムを暴走させ、動作停止処理プログラム3bを起動する。

動作停止処理プログラム3bは、盗難フラグ14が立てられているときには、この精算処理端末10の動作を停止させるために、あらかじめ指定されたメモリ3の領域のデータを無効とし、或はそれを消去し、かつ、メモリ3上に記憶されている入力データ処理プログラム3dを消去する。このことで採取されているデータについての処理、例えば、入出力ができなくなり、装置は正常な動作をしなくなる。また、盗難フラグ14が立てられていないときには、装着されたICカード20やメモリ3の入力データの記憶領域に無意味なデータを書込む処理をして正常な動作がなされないようにするか、処理プログラムを暴走させて正常な動作が行われないようにする。

ここで、時間監視回路8は、マイクロプロセッサ1により制御される。ICカード20が装着され、それが特定のコードを持つICカードであることをマイクロプロセッサ1が検出するとマイクロプロセッサ1は、時間監視回路8の時間監視動作を停止させ、かつ、時間計測値をリセットしてゼロに戻す。マイクロプロセッサ1は前記の特定のコードを持つICカードが装着されていない状態及びそのICカードが抜去された状態のいずれかを検出すると時間監視回路8に起動信号を送出して、時間監視回路8を動作させて時間計測を開始させる。なお、時間監視回路8の監視時間は、マイクロプロセッサ1から任意に設定可能であって、それが入力装置5からの入力により行われる。また、ICカードが特定のコードのものか否かは、そのICカードに与えられている識別コードを読出してこれと識別コード15と照合することにより行われる。

以上のような構成の精算処理端末10を、例えば、ICカードショッピング端末装置としてスーパーマーケットのレジに設置し、ICカードを所有する客のICカードに、商品購入代金データを書込み、キャッシュレスショッピングを行う端末として使用するとすることができる。この場合、ICカードに書込んだデータは、端末装置内に同

様なものが記憶され、バックアップしている。そして、後に客の銀行口座からその現金を引き落とす処理が行われる。そのため、このようなシステムでは、例えば、2時間に1回、レジ専任者等の責任者が専任者用ICカードを持って各レジを回り、端末装置に差し込んで端末装置内の前記のデータを含めて各種のデータをICカードに記録する処理が行われる。

このようなシステムにおいて、前記の時間監視回路8の設定時間がここでは2．5時間に設定されているとする。精算処理端末10は、例えば、2．5時間たっても責任者から特定のコードが記録されたICカードが挿入されないときには、その時間監視回路8からマイクロプロセッサ1に割込み信号が送出されて、対盗難処理プログラム3aが起動され、さらに動作停止処理プログラム3bが起動される。その結果、精算処理端末10の処理プログラムが暴走し、或は、メモリ3内や装着されたICカードに無意味なデータが書込まれる処理が行われる。そして、責任者を示す特定のICカードが差込まれた状態のときにのみ前記の時間監視が中止され、監視時間がゼロに戻る。なお、この場合、責任者を示す特定のICカードが差込まれた状態のときにのみ時間監視が中止されるので、夜間は所定の手続きにより時間監視を中止し、端末装置を金庫等にしまうようにするとよい。

ここで、この精算処理端末10が盗まれ、スーパマーケットから外部へと持ち出されると、端末装置内にバックアップしている購入代金データが解析されて、ICカード内の現金データが改ざんされる危険がある。そこで、これを防ぐためにスーパーマーケット内では信号送信装置21から特定の電波を放射し、これを精算処理端末10が端末装置内の板状のアンテナ8で常時受信するようなシステムとなっている。精算処理端末10が盗まれてスーパーマケット内から持ち出されると、精算処理端末10の電波強度検出回路7は、受信電波強度が一定レベル以下になったことを検出する。この検出信号による割込み処理でマイクロプロセッサ1により対盗難処理プログラム3aが起動され、さらに動作停止処理プログラム3bが起動されて、盗難フラグ14がセットされ、警報が鳴らされ、バックアップしている内部データと入力データ処理プログラム3dとが消去される。このようにすることにより内部データを読出して悪用されることはない。また、端末装置の処理プログラムの一部が消されているので、その端末装置は正常に動作しない。

このような精算処理端末10をICカード出退勤管理端末装置として利用することもできる。そこでその例を説明する。なお、この場合は、時間監視回路8の検出信号による割込みを電波強度検出回路7の割込みと同じものとして取り扱う。また、特定のICカードの装着の有無の検出して時間監視回路8が時間計測の解除を行うことに換えて入力装置5から特定の暗証コードを入力することにより時間計測の解除を行うものとする。

ICカード出退勤管理端末装置は、出退勤時にICカードを各自が差し込み、ICカードに出退勤時間等のデータを記録する。月に一度ICカードが集められ、出退勤時間等を読み取って労働時間等が計算される。また、前記と同様にICカード出退勤管理端末装置にはICカードに記録した出退勤データと同じデータがバックアップとして記録されている。この端末装置が盗まれるとICカード内の出退勤データが改ざんされる危険がある。これを防ぐため、本端末装置では、管理者が、3時間に1回暗証コードを入力装置5から入力する。出退勤管理端末装置は、内部で入力された暗証コードが時間監視回路8の監視時間を解除するコードか否かを内部に記憶されたコード（識別コード15に相当）と比較することで判定してこれらが一致したときに時間監視回路8を制御して計測した時間をリセットする。なお、ここでは時間監視回路8の設定時間が4時間に設定されているものとする。

この端末装置は、4時間の時間を監視し、4時間たっても正しい暗証コードが入力されないと、本端末装置は盗まれたと判定し、時間監視回路8

の割込み処理で対盗難処理プログラム３ａを起動する。そこで動作停止処理プログラム３ｂが起動されて警報が鳴らされる。これにより、盗んだ者が端末装置を所持していることが分かる。正しい暗証番号を入力したときに限って、端末装置の時間監視を初期に戻すことができる。なお、前記の例の場合も同様であるが、夜間は時間監視を停止するか、長い時間に設定する。これは、特定のコードで設定するようにできる。そこで、端末装置を金庫にしまうことができる。

以上説明してきたが、実施例では、特定のコードを有するＩＣカードに限って時間監視を初期に戻すようにしているが、これは、特定のＩＣカードによる必要はない。

また、正常動作停止手段として、実施例で挙げたもののほか、例えば、端末装置から入力されるキーの情報を無効とするような処理をしてもよい。

［発明の効果］

以上説明したように、この発明にあっては、時間監視手段の監視時間の開始をＩＣカードの抜去時点を基準とすることにより、ＩＣカードが所定時間の間装着されないときには時間監視手段の検出により正常動作停止手段が動作して、これによって、例えば、入力処理プログラムを消去し、記憶したデータを無効とすることで携帯用端末装置の正常なデータ処理が阻止されるので、盗難にあっても不正利用されなくても済む。

なお、前記のＩＣカードに換えて、入力装置から特定のコードを入力するようにして時間監視手段の時間計測を解除して初期状態に戻すようにしても同様の効果が得られる。

4.図面の簡単な説明

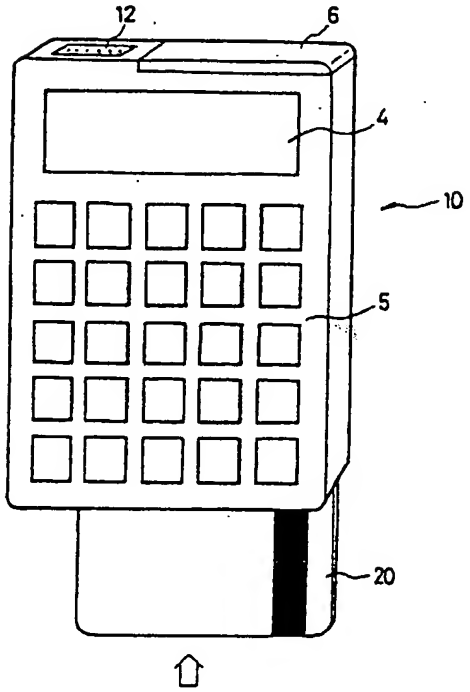
第１図は、この発明の携帯用端末装置の不正使用防止方式を適用したＩＣカード精算処理端末装置のブロック図であり、第２図は、その外観図である。

１…マイクロプロセッサ、２…クロック発振回路、３…メモリ、４…表示装置、５…入力装置、６…アンテナ、７…電波強度検出回路、８…時間監視回路、９…ＩＣカードインタフェース、１０…精算処理端末（ＩＣカード精算処理端末装置）、２０…ＩＣカード。

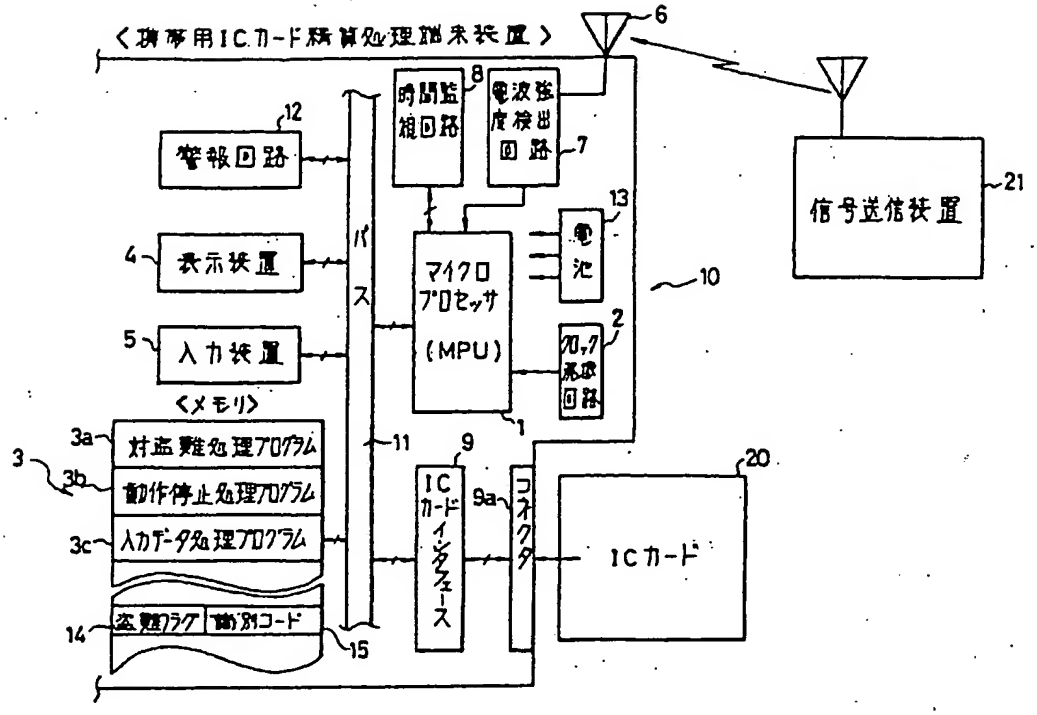
特許出願人　日立マクセル株式会社
株式会社日立製作所

代理人　弁理士　梶　山　佶　是
弁理士　山　本　富士男

第２図



第 1 図



第1頁の続き

⑤Int. Cl.⁵		識別記号		庁内整理番号
G 06 F	15/30	3 5 0		6798−5B
	15/74	3 4 0	A	7530−5B
G 06 K	17/00		S	6711−5B
G 08 B	13/00		Z	6376−5C
	21/00		D	7605−5C
	23/00		N	8621−5C

⑫発 明 者 小 寺 裕 司 大阪府茨木市丑寅1丁目1番88号 日立マクセル株式会社内

⑫発 明 者 山 下 廣 太 郎 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

⑫発 明 者 川 岡 明 宏 神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

⑫発 明 者 大 道 和 彦 大阪府茨木市丑寅1丁目1番88号 日立マクセル株式会社内

⑫発 明 者 小 島 徹 大阪府茨木市丑寅1丁目1番88号 日立マクセル株式会社内